IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

MT. RAINIER EMERGENCY PHYSICIANS, PLLC, RIVER ROCK WELLNESS, AND JENNA WOLFSON, individually and on behalf of all similarly situated persons,

Plaintiffs,

v.

CHANGE HEALTHCARE,

Defendant.

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Civil Action No. _____

CLASS REPRESENTATION

Jury Trial Demanded

Plaintiffs Mt. Rainier Emergency Physicians, PLLC, Dr. Michael P. Brook, River Rock Wellness, and Jenna Wolfson (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint against Change Healthcare, ("Change Healthcare" or "Defendant"), a Tennessee company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for failing to secure its systems and data from cyberattacks, including ransomware attacks. Defendant is a prominent provider of revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system. On February 21, 2024, Defendant suffered a ransomware attack, which prevented the Defendant's clients from conducting their routine and ordinary business, including

but not limited to, receiving payment for healthcare services rendered to the public ("Data Breach").

2. As a result of the Data Breach, and as further described below, Plaintiffs were unable to submit invoices to insurance companies for the services delivered to their clients, causing significant business interruption and lost revenues. Additionally, Plaintiffs have expended significant time and effort in an attempt to resolve the difficulties and mitigate the financial harms resulting from the breach.

PARTIES

3. Plaintiffs are, and at all times mentioned herein were: (i) healthcare entities that are customers of Defendant and use Defendant's business services, and (ii) these healthcare entities' principals, owners and shareholders.

4. Plaintiff Mt. Rainier Emergency Physicians, Pllc ("Mt. Rainier"), is a group practice located in Puyallup, Washington. Mt. Rainier provides staffing, including emergency room physicians and allied practitioners, to the MultiCare Good Samaritan Hospital in Puyallup, Washington. The hospital operates one of the busiest emergency departments in the country.

5. Dr. Michael P. Brook ("Brook") is an emergency medicine physician in Puyallup, Washington and is affiliated with MultiCare Good Samaritan Hospital. He received his medical degree from University of Saskatchewan College of Medicine and has been in practice for more than 20 years. He is the owner of Mt. Rainier.

6. Plaintiff River Rock Wellness ("River") is a therapy provider located in Fenton, California. River provides trauma-informed, holistic, and integrative care to individuals of various ages and with a variety of mental health and wellness needs.

7. Plaintiff Jenna Wolfson ("Wolfson") is a licensed social worker and the founder

and owner of River.

8. Defendant Change Healthcare is a Delaware corporation with its principal place of business headquartered in Nashville, Tennessee.

9. Since Change Healthcare shut down following the cyberattack, each of the Plaintiffs has been unable to obtain payment for the healthcare services provided to the vast majority of their patients and/or clients. Plaintiffs or their billing agents are unable to submit invoices to Change Healthcare, and, as a result, insurers are unable to cover any claims for services Plaintiffs provided. This caused, and continues to cause, Plaintiffs to suffer significant monetary losses and other harms.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and all conditions are met.

11. This Court has jurisdiction over Change Healthcare as it maintains its corporate headquarters in this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in the District and Change Healthcare is headquartered in this district.

GENERAL FACTUAL BACKGROUND

13. Change Healthcare is a subsidiary of UnitedHealth Group that enables data

transfers between providers, payers, and consumers within the healthcare system.[1]

14. Change Healthcare operates the largest administrative information exchange in the United States. Change Healthcare's products and services are used by more than 1,200 government and commercial payers; 6,000 hospitals; one million physicians and 2,400 payer connections.[2]

15. Change Healthcare handles more than 15 billion healthcare transactions totaling more than $1.5 trillion a year and represents "a critical pipeline connecting health-care organizations with insurance companies who review their claims, pay for their services and determine the costs of care for patients.[3,4]

16. In effect, Change Healthcare represents a utility, with which nearly all healthcare providers in the country interact, in order to exchange their patients' personal health information and financial information, and to obtain payment for services provided to their patients. Its status as a critical piece of national infrastructure which handles highly sensitive information should have alerted Change to the risk of cyber criminals attempting to hijack it for financial gain. However, Change took inadequate, if any, measures to prevent this occurrence. This risk materialized when Change suffered the Data Breach on February 21, 2024, and which has not been remedied to date.

17. Because of its involvement with electronic personal health information ("PHI"), Change Healthcare is both a "Covered Entity" and a "Business Associate" as defined under the

[1] Joseph Menn and Daniel Gilbert, U.S. prescription drug market in disarray as ransomware gang attacks, The Washington Post, (March 2, 2024) https://www.washingtonpost.com/technology/2024/03/01/prescription-drug-hack-alphv/ (last visited on March 8, 2024).
[2] Change Healthcare, Medical Network https://www.changehealthcare.com/medical-network (last visited on March 8, 2024).
[3] Dan Diamond and Daniel Gilbert, Officials rush to help hospitals, doctors affected by Change Healthcare hack, The Washington Post (March 5, 2024) https://www.washingtonpost.com/health/2024/03/05/change-healthcare-insurance-hack-hhs-plan/ (last visited on March 8, 2024).
[4] Steve Alder, Change Healthcare Confirms Blackcat Ransomware Attack as Systems Brought Back Online, The HIPAA Journal (March 2, 2024) https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

rules and regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 CFR Parts 160 to 164). The HIPAA "Security Rule," published in 2003, addresses the requirement that both Covered Entities and Business Associates adopt security procedures to assure the confidentiality, integrity, and availability of personal health care information, or PHI (45 CFR Part 160 and Subparts A and C of Part 164).[5]

18. Change Healthcare's own "Privacy Notice", in the Security and Data Retention section, mirrors the language of its HIPAA obligations as its website states that: "We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse."[6]

19. As a condition of receiving its services, Change Healthcare requires that its customers entrust it with highly sensitive information, including their patients' and customers' PHI.

RANSOMWARE THREATENS HEALTHCARE

14. Ransomware is a subset of malware in which the data on a victim's computer, or network, is locked, typically by encryption, and where payment is demanded as a condition of providing the decryption key to unlock the encrypted data and once again make that data available

[5] The Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited March 3, 2024), *emphasis added*.
[6] Change Healthcare's Security Policy, https://www.changehealthcare.com/privacy-notice (last visited March 3, 2024).

to the victim.[7] The motive for ransomware attacks is nearly always monetary, and the demanded payment is almost always in some form of crypto-currency, typically Bitcoin.[8]

15. Various forms of ransomware have been used to attack corporate as well as individual user systems since as early as 2013. The Cryptolocker strain of ransomware posed as a Trojan horse (malware contained or incorporated within otherwise legitimate-seeming websites, applications, or attachments to emails or messages). In 2017, the WannaCry ransomware attacked and encrypted more than 300,000 Microsoft Windows systems globally, demanding payment in Bitcoin in exchange for the data decryption key. WannaCry's mode of operation closely follows ransomware's general methodology:

> When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 in bitcoin within three days, or $600 within seven days.[9]

16. While the extortionist's payment demand is relatively small (ranging between hundreds of dollars to tens of thousands of dollars), the damage wreaked on enterprise and other users' systems reaches hundreds of millions of dollars and more.

17. Unlike a data breach, whose seriousness results from the exfiltration and criminal usage of personally identifiable information or personal health care information, a ransomware attack renders data stored within a computer network or individual computer both unreadable and

[7] Ransomware, http://searchsecurity.techtarget.com/definition/ransomware (last visited March 2, 2024)
[8] *Id.*
[9] WannaCry Ransomware Attack, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (last visited March 2, 2024)

completely inaccessible to the enterprise or computer user. In the case of a health care products or services provider, the consequences can mean life or death.

18. Accordingly, hospitals, other healthcare related facilities and goods and services providers in the healthcare field, such as the Defendant, are especially attractive targets for ransomware. While no sensitive or health information is disseminated, the risks to patient treatment, health, and safety are significantly increased because of the serious and even life-threatening consequences presented by even a short-lived interruption of healthcare services. One example of this is Hollywood Presbyterian Medical Center in Los Angeles, who in early 2016 was the victim of a ransomware attack and opted to pay $17,000 in Bitcoin to retrieve the key to unlock its data.[10]

19. Other healthcare goods and services providers are not immune from ransomware attacks. In mid-2017, pharmaceutical giant Merck was the subject of the ransomware strain known as "NotPetya." Merck's business was brought to a virtual halt, and the cost to Merck, as of October 2017, amounted to more than $300 million, including more than $175 million in lost business,[11] with the costs to insurers having been estimated at $275 million.[12]

20. It has been reported that the Blackcat ransomware gang has operated since at least as early as November 2021[13], and has become the second most prolific ransomware-as-a-service

[10] Richard Winton, Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating, The LA Times (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (last visited March 18, 2024)
[11] Patrick Howell O'Neill, NotPetya Ransomware Cost Merck More than $310 Million, Cyber Scoop (Oct. 27, 2017), https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/ (last visited March 18, 2024).
[12] Reuters Staff, Merck Cyber Attack May Cost Insurers $275 Million: Verisk's PCS, Reuters (Oct. 19, 2017), https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP (last visited March 18, 2024).
[13]Blackberry, What Is BlackCat Malware?, https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat (last visited March 18, 2024).

criminal group in the world. Blackcat affiliates gain initial access to networks by primarily leveraging compromised user credentials.[14]

21. It was widely known that ransomware attacks were a threat to healthcare-related entities, in 2024. Indeed, the first ransomware attack was reported to occur in 1989 and involved a healthcare provider.[15]

THE FEBRUARY 2024 RANSOMWARE EVENT AT CHANGE HEALTHCARE

29. Beginning on or about February 21, 2024, a ransomware gang known as Blackcat – also known as AlphV – attacked, compromised, and crippled Change Healthcare's data centers in Nashville, Tennessee, preventing Plaintiffs from submitting invoices for payment to insurance companies for the services delivered to clients. The attack has impacted electronic prescription and invoice processing for millions of U.S. residents.[16]

30. UnitedHealth confirmed with the U.S. Securities and Exchange Commission (SES) that Change Healthcare had experienced a cyberattack.[17]

31. On February 22, 2024, Change Healthcare disclosed that its system had been attacked and infected by the Blackcat ransomware, resulting in the encryption of patient health-related information used to conduct Change Healthcare's business.[18]

---

[14] Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant, U.S. Department of Justice, https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant (December 19, 2023), (last visited March 18, 2024).

[15] Nate Lord, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, Digital Guardian (Dec. 7, 2017), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time (last visited March 18, 2024).

[16] Joseph Menn and Daniel Gilbert, U.S. prescription drug market in disarray as ransomware gang attacks, The Washington Post, (March 2, 2024) https://www.washingtonpost.com/technology/2024/03/01/prescription-drug-hack-alphv/ (last visited March 18, 2024).

[17] Steve Alder, Change Healthcare Confirms Blackcat Ransomware Attack as Systems Brought Back Online, The HIPAA Journal (March 2, 2024) https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ (last visited March 18, 2024).

[18] Information on the Change Healthcare Cyber Response, United Healthcare Group (March 4, 2024) https://www.unitedhealthgroup.com/ns/changehealthcare.html (last visited March 18, 2024).

32. As a result of the cyberattack, Change Healthcare shut down the majority of its network. Patients have been unable to get information on whether insurance will cover a treatment or prescription.[19] In addition, the cyber attack has impacted health care organizations and services providers, including but not limited to the Plaintiffs, by preventing them from invoices for payment to their patients' or clients' insurance companies through Change.

33. In short, because of Change's central and mission-critical role in the U.S. healthcare system, a significant proportion of U.S. hospitals, medical practitioners and allied professionals are unable to receive payment for services provided to privately insured persons since the February 21, 2024, cyber attack. This disruption, and the associated financial and other harms, continue to this day.

34. What makes the Blackcat attack so pernicious is that by encrypting (and hobbling) key components of Change Healthcare's network, it also hobbled Change Healthcare's ability to conduct its business – the Change Healthcare's Professional EHR System – preventing it from processing claims from a large number of U.S. hospitals and health care providers.[20]

35. Healthcare industry knowledge and awareness of the widespread issues with Blackcat ransomware and the actors who operate it dates back to November 2021 at the latest.[21] Change Healthcare disregarded Plaintiffs' and Class Members' rights by intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to implement,

---

[19] Daniel Gilbert, Dan Diamond, Christopher Rowland and Kim Bellware, Health-care hack spreads pain across hospitals and doctors nationwide, The Washington Post, (March 3 3024) https://www.washingtonpost.com/business/2024/03/03/change-health-care-hack-hospitals/ (last visited March 18, 2024).

[20] Steve Alder, Change Healthcare Confirms Blackcat Ransomware Attack as Systems Brought Back Online, The HIPAA Journal (March 2, 2024) https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ (last visited March 18, 2024)

[21] Blackberry, What Is BlackCat Malware? https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat, (last visited March 4, 2024).

monitor, and audit its data systems, which could have prevented or minimized the effects of the Blackcat ransomware attack it experienced in February 2024.

36. Ransomware attacks are Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[22]

37. The Blackcat attack on Change Healthcare's systems and data is also considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.[23]

38. As of the filing of this Complaint, Change Healthcare has not disclosed the full nature and extent of the attack on its systems; however, upon information and belief, the full functionality of its services has not yet been restored. Furthermore, Change Healthcare has not mitigated the impact of the breach on the Plaintiffs and the Class, resulting in continued inability to collect payment for their services and associated severe and growing harm.

[22] FACT SHEET: Ransomware and HIPAA, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last visited March 2, 2024).
[23] *Id.*

PLAINTIFFS AND THE CLASS SUFFERED DAMAGES

25. Plaintiffs and the Class are: (a) purchasing users of Change Healthcare's products and services and (b) these purchasing users' owners, shareholders or principals.

26. In their everyday practice, and as an integral part of their business, Plaintiffs and the Class place significant reliance on their ability to access and transact with the products and services provided by Change Healthcare.

27. As a direct and proximate result of Change Healthcare's wrongful acts and omissions, Plaintiffs and the Class suffered, and continue to suffer, economic damage and other actual harm, including monetary losses arising from significant business interruption and disruption, together with expenses incurred in attempts to mitigate such business interruption and disruption.

28. As of the date of the filing of this Complaint, Plaintiffs and the Class continue to experience significant business interruption and disruption as a direct and proximate result of their inability to, among others: access and transact with Change Healthcare's products and services; submit invoices for services rendered to their patients and clients through their billing agents; and submit electronic prescriptions. Change Healthcare's wanton, willful, and reckless disregard caused a complete and total interruption of service, and further caused Plaintiffs and the Class monetary and other damages.

29. Change Healthcare failed to implement appropriate processes that could have prevented or minimized the effects of the Blackcat ransomware attack.

30. Plaintiffs acted in reasonable reliance on Change Healthcare's misrepresentations and omissions regarding the security of its products and services, and would not have purchased Change Healthcare's products and/or services had they known that Change Healthcare did not take

all necessary precautions to protect itself from cyberattack, including ransomware attacks. Plaintiffs and the Class would not have gone through with a purchase had they known that the use of Change Healthcare's products was accompanied by an unreasonable risk of business disruption, interruption and monetary loss.

CLASS ACTION ALLEGATIONS

31. Plaintiffs seek relief in their individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of the following subclasses (together, the "Nationwide Class"):

> All Change Healthcare customers located in the United States who were affected by an interruption of service due to the ransomware attack which occurred on February 21, 2024 (the "Entity Subclass").
>
> All individuals who are principals, shareholders or owners of members of the Entity Subclass ("Individual Subclass").

32. Excluded from the above Nationwide Class is Change Healthcare, including any entity in which Change Healthcare has a controlling interest, is a parent or subsidiary, or which is controlled by Change Healthcare, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Change Healthcare. Also excluded are the judges and court personnel in this case and any members of their immediate families.

33. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Nationwide Class are so numerous that the joinder of all members is impractical. While the exact number of Class members

is unknown to Plaintiffs at this time, Change Healthcare provides services to 60,000 pharmacies,[24] 6000 hospitals and numerous other healthcare services providers.[25]

34. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Nationwide Class, which predominate over any questions affecting only individual Nationwide Class members. These common questions of law and fact include, without limitation:

a. Whether Change Healthcare failed to implement, monitor and audit adequate processes to timely detect, prevent, or mitigate a cyberattack;

b. Whether Change Healthcare's failures and omissions constitute a breach of contract;

c. Whether Change Healthcare's failures and omissions constitute negligence, or negligence *per se*;

d. Whether Change Healthcare violated the Tennessee Consumer Protection Act of 1977 ("TCPA") by failing to comply with the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

e. Whether Change Healthcare violated the TCPA by failing to comply with the HIPAA Security Rule; to wit, by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

[24] Sarah Lewis, Change Healthcare, Tech Target, https://www.techtarget.com/searchhealthit/definition/Change-Healthcare#:~:text=Network%20solutions%2D%20Change%20Healthcare%20offers,all%20government%20and%20commercial%20payers. (last visited on March 8, 2024).
[25] Change Healthcare, "Medical Network" https://www.changehealthcare.com/medical-network (last visited on March 8, 2024).

f. Which security procedures and which data-breach notification procedures should Change Healthcare be required to implement as part of any injunctive relief ordered by the Court;

g. Whether Change Healthcare has an implied contractual obligation to use reasonable security measures;

h. Whether Change Healthcare has complied with any implied contractual obligation to use reasonable security measures;

i. What security measures, if any, must be implemented by Change Healthcare to comply with its implied contractual obligations;

j. Whether Change Healthcare's acts and/or omissions in respect of the data-breach it suffered on or about February 21, 2024, caused financial harm to the Nationwide Class Members;

k. What the nature of the relief should be, including damages and/or equitable relief, to which Plaintiffs and the Nationwide Class members are entitled.

35. All members of the proposed Nationwide Class are readily ascertainable. Change Healthcare has access to the addresses and other contact information for members of the Nationwide Class, which can be used for providing notice to many Nationwide Class members.

36. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Nationwide Class members because Plaintiffs were denied the ability to seek reimbursement for their services from their patients' or clients' insurers, like every other class member.

37. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Nationwide Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation.

38. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Nationwide Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

39. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Change Healthcare's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Nationwide Class.

40. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Change Healthcare has acted or has refused to act on grounds generally applicable to the Nationwide Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole.

COUNT I – NEGLIGENCE AND NEGLIGENCE *PER SE*

(On Behalf of Plaintiffs and the Nationwide Class)

41. Plaintiffs repeat and fully incorporate all factual allegations contained in paragraphs 1 through 40 as if fully set forth herein.

42. Change Healthcare owed a duty to Plaintiffs and Nationwide Class Members to exercise reasonable care to safeguard its systems and data from cyberattack, including ransomware attacks.

43. This duty of care is distinct from any contractual obligation the Defendant owed the Entity Subclass (as discussed below), and the damages arising from its breach are distinct from

the Nationwide Class' damages sought in respect of its statutory, unjust enrichment and breach of contract claims.

44. Change Healthcare is both a Covered Entity as well as a Business Associate; and as such, has a duty to protect PHI in accordance with the provision of HIPPA.

45. Change Healthcare breached its duties by failing to implement, monitor, and audit the security of its data and systems, resulting in a ransomware attack that significantly impeded and/or prevented its clients' ability to conduct business.

46. Change Healthcare violated its duties and its obligations under HIPAA as a Covered Entity and a Business Associate by reason of the infiltration of ransomware into its systems and data.

47. Neither Plaintiffs nor the Class contributed to the Data Breach as described in this Complaint.

48. As a direct and proximate result of Change Healthcare's conduct, Plaintiffs and the Nationwide Class suffered damages including, but not limited to, disruption and interruption of its business and everyday provision of services to patients.

49. Change Healthcare's acts and omissions as alleged herein were willful, wanton, and with reckless disregard for the rights of Plaintiffs and the Nationwide Class.

50. Change Healthcare's acts and omissions in violating HIPAA constitute negligence *per se* because it failed to maintain the integrity and availability of PHI.

51. As a result of Change Healthcare's negligence, and negligence *per se*, Plaintiffs and the Nationwide Class suffered damages, including costs incurred as a result of business interruption and disruption, together with other damages as may be shown at trial.

COUNT II – BREACH OF CONTRACT

(On Behalf of Plaintiffs and the Entity Subclass)

52. Plaintiffs incorporate the factual allegations contained in Paragraphs 1 through 40 as if fully set forth herein.

53. Change Healthcare entered into contracts with Plaintiffs Mt. Rainier and River, and the Entity Subclass.

54. Change Healthcare agreed to provide its specialized services in a professional and workmanlike manner. Implicit in performing these contractual duties is an obligation to reasonably safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients.

55. In particular, in its contracts with the Plaintiffs and other Entity Subclass members, Change Healthcare undertook to "implement and use appropriate administrative, physical, and technical safeguards and, as of September 23, 2013, comply with applicable Security Regulation requirements with respect to electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by this BA Agreement."

56. Change Healthcare breached its contracts with Plaintiffs Mt. Rainier and River, and Entity Subclass members by failing to reasonably safeguard its systems and data from cyberattack, including ransomware attacks.

57. As a direct and proximate result of Change Healthcare's contract breaches, Plaintiffs Mt. Rainier and River, and the Entity Subclass sustained actual losses and damages including, but not limited to, complete interruption and disruption of its ability to obtain reimbursement for services provided to their patients or clients.

COUNT III – UNJUST ENRICHMENT

(On behalf of Plaintiffs and the Nationwide Class)

58. Plaintiffs repeat and incorporate the allegations contained in paragraphs 1 through 40 as if fully set forth herein.

59. Plaintiffs and the Nationwide Class conferred a benefit on Change Healthcare when they provided payment to Change Healthcare for the sale of its products and services.

60. In exchange for, and in consideration of, Plaintiffs and Nationwide Class members providing payment for Change Healthcare's products and services, Change Healthcare was required to, and Plaintiffs and the Nationwide Class expected Change Healthcare to, implement reasonable security policies and procedures that would have detected, prevented, or mitigated a Blackcat ransomware attack.

61. Change Healthcare states that it devotes "significant resources" to protect PHI, a portion of which is derived from the benefit conferred by the contractual payments made by Plaintiffs and the Class to Change Healthcare.

62. As a result of Change Healthcare's acts and omission as alleged herein, Change Healthcare has been unjustly enriched to the extent that any portion of such payments comprises spending for adequate security not provided.

COUNT IV – VIOLATION OF TENNESSEE CONSUMER PROTECTION ACT OF 1977

(On behalf of Plaintiffs and the Nationwide Class)

63. Plaintiffs repeat and incorporate the allegations contained in paragraphs 1 through 40 as if fully set forth herein.

64. TCPA provides that one of its statutory purposes is "to protect consumers and legitimate business enterprises from those who engage in unfair or deceptive acts or practices in the conduct of any trade or commerce in part or wholly within this state." (TN Code §47-18-102(2)).

65. Change Healthcare, operating through its Tennessee headquarters, engaged in unfair or deceptive acts or practices, which constitute unlawful acts or practices in the conduct of trade or commerce, in violation of TCPA, see: TN Code § 47-18-104, including but not limited to the following:

a. Fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

b. Misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an

enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients and to prevent infiltration of the security system so as to safeguard PHI from unauthorized access; and

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact reasonable security practices to safeguard its systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday provision of services to its clients.

66. As a direct and proximate result of Change Healthcare's deceptive trade practices, Plaintiffs and the Nationwide Class suffered injuries, including but not limited to, complete interruption and disruption of its business of providing services to patients or complete denial of service and the corresponding inability to operate their business of providing services to patients.

67. The above unfair and deceptive practices and acts by Change Healthcare were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that

Plaintiffs and the Nationwide Class could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

68. Change Healthcare knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of a ransomware attack, data breach, or theft was high. Change Healthcare's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class.

69. By the authority of TN Code §47-18-109, "any person who suffers an ascertainable loss of money or property," as a result of unfair or deceptive acts or practices of another, may bring an action to recover actual damages.

70. Pursuant to the same provision, the court may award three times the actual damages sustained if it finds that the use or employment of the unfair or deceptive act or practice was a willful or knowing violation of TCPA. (TN Code §47-18-109(a)(3))

71. Further, TCPA provides that no provision of the act may be "limited by contract, agreement or otherwise". (TN Code §47-18-113(a))

72. Plaintiffs and the Nationwide Class seek relief under Tenn. Code §47-18-109, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

73. To the extent TCPA purports to limit the availability of class actions filed in Federal Courts for relief under TCPA, it is preempted by Rule 23 of the Federal Rules of Civil Procedure.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Change Healthcare as follows:

a. For an Order certifying the Nationwide Class as defined herein, and appointing:

   i. Plaintiffs Mt. Rainier and River to represent the Entity Subclass;

   ii. Plaintiffs Brook and Wolfson to represent the Individual Subclass; and

   iii. Plaintiffs' Counsel to represent the Entity Subclass, Individual Subclass and the Nationwide Class;

b. For equitable relief compelling Change Healthcare to utilize appropriate methods and policies with respect to ransomware protection;

c. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Change Healthcare's wrongful conduct;

d. For an award of actual damages and compensatory damages, in an amount to be determined;

e. For an award of damages sustained by the Class, trebled, in accordance with TN Code § 47-18-109(a)(3);

f. For an award of pre-judgment and post-judgment interest as allowed by law;

g. For an award of costs of suit and attorneys' fees, as allowable by law; and

h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

DATED: March 20, 2024

Respectfully submitted,

/s/ Kathryn E. Barnett
KATHRYN E. BARNETT
Tennessee Bar No. 015361
MORGAN & MORGAN
810 Broadway Ste. 105
Nashville, TN 37203-3808
Telephone: (615) 490-0943
kbarnett@forthepeople.com

JOHN A. YANCHUNIS*
Florida Bar No. 324681
jyanchunis@ForThePeople.com
RONALD PODOLNY*
New York Bar No. 4772232
ronald.podolny@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

**pro hac vice to be filed*

Attorneys for Plaintiffs and the Proposed Class